

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2001-44992  
(P2001-44992A)

(43) 公開日 平成13年2月16日 (2001.2.16)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
H 0 4 L 12/22		H 0 4 L 11/26	
G 0 6 F 15/00	3 1 0	G 0 6 F 15/00	3 1 0 A
	3 3 0		3 3 0 A
15/16	6 2 0	15/16	6 2 0 A
15/177	6 7 0	15/177	6 7 0 C

審査請求 未請求 請求項の数34 O L (全 18 頁) 最終頁に続く

(21) 出願番号 特願2000-148684 (P2000-148684)

(22) 出願日 平成12年5月19日 (2000.5.19)

(31) 優先権主張番号 09/315636

(32) 優先日 平成11年5月20日 (1999.5.20)

(33) 優先権主張国 米国 (US)

(71) 出願人 596077259

ルーセント テクノロジーズ インコーポ  
レイテッド  
Lucent Technologies  
Inc.

アメリカ合衆国 07974 ニュージャージ  
ー、マレーヒル、マウンテン アベニュー  
600-700

(74) 代理人 100081053

弁理士 三俣 弘文

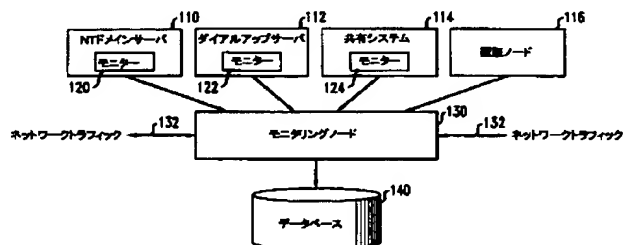
最終頁に続く

(54) 【発明の名称】 ネットワーク動作方法、ネットワークノード、ネットワーク装置、及び通信ネットワーク

(57) 【要約】

【課題】 データネットワークの利用状況を特定のユーザに関連付ける、より改善された技法を提供することが本発明の課題である。

【解決手段】 本発明に従って、ネットワークモニタリングノードがネットワーク認証ソースから認証データを受信する。認証データは、通常、認証済みユーザの識別及び当該ユーザに係る現時点でのネットワークアドレスを含んでいる。この認証データはモニタリングノードに蓄積される。その後、ネットワークアドレスを含むデータパケットの受信にตอบสนองして、モニタリングノードは、データパケットのネットワークアドレスをストアされたユーザのネットワークアドレスと比較することによって、ユーザをデータパケットに関連付ける。モニタリングノードは、ユーザの利用状況データを生成し、ユーザの利用状況データをデータベースに供給する。この利用状況データは、与えられたユーザに関して集積される。



## 【特許請求の範囲】

【請求項 1】 ネットワークノードを動作させる方法において、当該方法が、ユーザをネットワークアドレスに関連付けるデータを少なくとも一つのネットワーク認証ソースから受信する段階；ここで、前記データはユーザの前記認証に即時応答して受信される；ネットワークアドレスを有するデータパケットを受信する段階；及び、前記ネットワークアドレスをユーザをネットワークアドレスに関連付ける前記データと比較することによって前記データパケットに関連付けられるユーザを実質的にリアルタイムで決定する段階；を有することを特徴とするネットワーク動作方法。

【請求項 2】 前記方法が、さらに、前記データパケットに関連付けられるサービスを実質的にリアルタイムで決定する段階；を有することを特徴とする請求項 1 に記載のネットワーク動作方法。

【請求項 3】 前記方法が、さらに、集積されるユーザ利用状況データをデータベースにストアする段階；を有することを特徴とする請求項 1 に記載のネットワーク動作方法。

【請求項 4】 前記少なくとも一つの認証ソースが、認証サーバを含んでいることを特徴とする請求項 1 に記載のネットワーク動作方法。

【請求項 5】 前記少なくとも一つの認証ソースが、設置された認証ノードを含んでいることを特徴とする請求項 1 に記載のネットワーク動作方法。

【請求項 6】 少なくとも一つのネットワーク認証ソースからユーザ認証データを受信する段階；ここで、前記ユーザ認証データはユーザの認証に即時に응答して受信される；データパケットを受信する段階；及び、ユーザを前記受信されたデータパケットに関連付ける目的で前記受信されたデータパケットを前記ユーザ認証データに対して実質的にリアルタイムで比較することによって利用状況データを生成する段階；を有することを特徴とするネットワーク動作方法。

【請求項 7】 前記方法が、さらに、前記データパケットに関連付けられるサービスを実質的にリアルタイムで決定する段階；を有することを特徴とする請求項 6 に記載のネットワーク動作方法。

【請求項 8】 前記方法が、さらに、集積されるユーザ利用状況データをデータベースにストアする段階；を有することを特徴とする請求項 6 に記載のネットワーク動作方法。

【請求項 9】 前記方法が、さらに、前記データパケットに関連付けられた前記ユーザに依存して前記データパケットを相異なった方式で処理する段階；を有することを特徴とする請求項 6 に記載のネットワーク動作方法。

【請求項 10】 前記方法が、さらに、前記利用状況データに基づいてユーザに課金する段階；を有することを特徴とする請求項 6 に記載のネットワーク動作方法。

【請求項 11】 前記方法が、さらに、前記利用状況データに基づいてネットワークサービス品質を実現する段階；を有することを特徴とする請求項 6 に記載のネットワーク動作方法。

【請求項 12】 ネットワーク利用状況データを生成する方法において、当該方法が、少なくとも一つのネットワーク認証ソースからユーザ認証データを受信する段階；ここで、前記ユーザ認証データはユーザの認証に即時に응答して受信される；ネットワークトラフィックをモニタする段階；及び、前記ネットワークトラフィックを前記ユーザ認証データと比較することによって前記ネットワークトラフィックのある部分を特定のユーザに対して実質的にリアルタイムに関連付ける段階；を有することを特徴とするネットワーク動作方法。

【請求項 13】 前記方法が、さらに、前記ネットワークトラフィックのある部分を特定のサービスに対して実質的にリアルタイムに関連付ける段階；を有することを特徴とする請求項 12 に記載のネットワーク動作方法。

【請求項 14】 前記方法が、さらに、集積されるユーザ利用状況データをデータベースにストアする段階；を有することを特徴とする請求項 12 に記載のネットワーク動作方法。

【請求項 15】 前記方法が、さらに、前記ネットワークトラフィックの前記部分に関連付けられた前記ユーザに依存して前記ネットワークトラフィックの前記部分を相異なった方式で処理する段階；を有することを特徴とする請求項 12 に記載のネットワーク動作方法。

【請求項 16】 前記方法が、さらに、前記ネットワーク利用状況データに基づいてユーザに課金する段階；を有することを特徴とする請求項 12 に記載のネットワーク動作方法。

【請求項 17】 前記方法が、さらに、前記ネットワーク利用状況データに基づいてネットワークサービス品質を実現する段階；を有することを特徴とする請求項 12 に記載のネットワーク動作方法。

【請求項 18】 少なくとも一つのネットワーク認証ソースからユーザ認証データを受信する目的；ここで、前記ユーザ認証データはユーザの認証に即時に응答して受信される；及び、ネットワークトラフィックを受信する目的；で使用される少なくとも一つのネットワークインターフェース；前記受信されたユーザ認証データをストアするメモリ；及び前記ネットワークトラフィックのある部分を特定のユーザに関連付ける目的で前記ネットワークトラフィックを前記ストアされたユーザ認証データと実質的にリアルタイムで比較するように、ストアードプログラムコードに従って動作するプロセッサ；を有することを特徴とするネットワークノード。

【請求項 19】 前記プロセッサが、さらに、ストアードプログラムコードに従って前記ネットワークトラフィックのある部分に関連付けられたサービスを実質的にリ

## 3

リアルタイムで決定するように機能すること；を特徴とする請求項 18 に記載のネットワークノード。

【請求項 20】 ネットワーク利用状況データ生成装置において、当該装置が、少なくとも一つのネットワーク認証ソースからユーザ認証データを受信する手段；ここで、前記ユーザ認証データはユーザの認証に即時にตอบสนองして受信される；ネットワークトラフィックをモニタする手段；及び、前記ネットワークトラフィックを前記ユーザ認証データと比較することによって前記ネットワークトラフィックのある部分を特定のユーザに対して実質的にリアルタイムに関連付ける手段；を有することを特徴とするネットワーク装置。

【請求項 21】 前記装置が、さらに、前記ネットワークトラフィックのある部分を特定のユーザに実質的にリアルタイムに関連付ける手段；を有することを特徴とする請求項 20 に記載のネットワーク装置。

【請求項 22】 前記装置が、さらに、集積される利用状況データをデータベースにストアする手段；を有することを特徴とする請求項 20 に記載のネットワーク装置。

【請求項 23】 ユーザがデータを送受信する目的で利用する通信ネットワークにおいて、当該ネットワークが、

- 1) ユーザ認証に即時ตอบสนองしてユーザ認証データを送信する少なくとも一つのネットワーク認証ソース；及び、
- 2) a) ユーザ認証データを少なくとも一つのネットワーク認証ソースから受信する目的；及びデータネットワークトラフィックを受信する目的；で用いられる少なくとも一つのネットワークインターフェース；
- b) 前記受信されたユーザ認証データをストアするメモリ；及び、
- c) 前記ネットワークトラフィックのある部分を特定のユーザに関連付ける目的で前記ネットワークトラフィックを前記ストアされたユーザ認証データと実質的にリアルタイムで比較することによってユーザ利用状況データを生成するプロセッサ；を有することを特徴とする通信ネットワーク。

【請求項 24】 前記通信ネットワークが、さらに、集積されるユーザ利用状況データをストアするデータベース；を有することを特徴とする請求項 23 に記載の通信ネットワーク。

【請求項 25】 前記通信ネットワークが、さらに、前記ユーザ利用状況データを受信し、利用状況に少なくとも一部分基づいてユーザに課金する課金アプリケーション；を有することを特徴とする請求項 23 に記載の通信ネットワーク。

【請求項 26】 前記通信ネットワークが、さらに、前記ユーザ利用状況データを受信し、前記ユーザ利用状況データに少なくとも一部分基づいてユーザに対してサービス品質を提供するサービス品質アプリケーション；を

## 4

有することを特徴とする請求項 23 に記載の通信ネットワーク。

【請求項 27】 前記通信ネットワークが、さらに、前記ユーザ利用状況データを受信し、前記ユーザ利用状況データに少なくとも一部分基づいてネットワークトラフィックを制限するファイアウォール；を有することを特徴とする請求項 23 に記載の通信ネットワーク。

【請求項 28】 ユーザがデータを送受信する目的で利用する通信ネットワークにおいて、当該ネットワークが、

- 1) ユーザによるデータ転送の開始に即時ตอบสนองしてユーザ認証データを生成かつ送信するプログラムコードを有するソケットライブラリを有する、複数の同時ユーザを有する共用コンピュータシステム；
- 2) a) ユーザ認証データを前記共用コンピュータシステムから受信する目的；及びデータネットワークトラフィックを受信する目的；で用いられる少なくとも一つのネットワークインターフェース；
- b) 前記受信されたユーザ認証データをストアするメモリ；及び、
- c) 前記ネットワークトラフィックのある部分を特定のユーザに関連付ける目的で前記ネットワークトラフィックを前記ストアされたユーザ認証データと実質的にリアルタイムで比較することによってユーザ利用状況データを生成するプロセッサ；を有することを特徴とする通信ネットワーク。

【請求項 29】 ユーザによるデータ転送の開始に即時ตอบสนองして共用コンピュータシステムからユーザ認証データを受信する段階；データパケットを受信する段階；及び、ユーザを前記受信されたデータパケットと関連付ける目的で前記受信されたデータパケットを前記ユーザ認証データと実質的にリアルタイムで比較することによって利用状況データを生成する段階；を有することを特徴とするネットワーク動作方法。

【請求項 30】 前記方法が、さらに、前記データパケットに関連付けられたサービスを実質的にリアルタイムで決定する段階；を有することを特徴とする請求項 29 に記載のネットワーク動作方法。

【請求項 31】 前記方法が、さらに、集積される利用状況データをデータベースにストアする段階；を有することを特徴とする請求項 29 に記載のネットワーク動作方法。

【請求項 32】 前記方法が、さらに、前記データパケットに関連付けられたユーザに基づいて前記ネットワークにおける前記データパケットを相異なった方式で処理する段階；を有することを特徴とする請求項 29 に記載のネットワーク動作方法。

【請求項 33】 前記方法が、さらに、前記利用状況データに基づいてユーザに課金する段階；を有することを特徴とする請求項 29 に記載のネットワーク動作方法。

【請求項 34】 前記方法が、さらに、前記利用状況データに基づいてネットワークサービス品質を提供する段階；を有することを特徴とする請求項 29 に記載のネットワーク動作方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はデータネットワークに関し、特に、ネットワークの利用を特定のユーザに関連付ける技法に関する。

【0002】

【従来の技術】 歴史的には、データネットワークに係るユーザ固有の利用状況に関するデータの収集は、ネットワーク設計者の主たる対象ではなかった。例えば、インターネットの利用は伝統的にユーザに対して無料であり、実際の費用は種々の研究機関、企業、及び政府関係機関の予算に吸収されてきた。よって、ネットワークのモニタリング及びプランニングに関して大量のネットワーク利用状況データが集積されてきたにもかかわらず、ユーザ固有のネットワーク利用状況情報を収集する必要はほとんど無かった。

【0003】 しかしながら、一般的に言えばデータネットワーク、特にインターネットが成長して発展するに連れ、ユーザ固有の利用状況情報に係る必要性が生じてきている。この必要性はいくつかの要因に関連付けられる。第一に、ネットワーク事業者は、ネットワークサービスの提供に係るコストを回収する方法を必要としている。現在の利用無制限の様な利用料金方式は、より多くの革新的かつ差別化されたサービスを提供する際の障害になっている。従来技術に係る音声電話ネットワークにおいて用いられてきたような、利用状況に基づくより身近な料金モデルを採用することにより、サービスプロバイダが革新的なサービスを提供すること及びそれによって課金することが可能になる。

【0004】 第二に、サービス品質に係る要求の増大は利用状況に基づく情報の必要性を示唆している。伝統的には、データネットワークはベスト・エフォートというサービスポリシーの下で運営されており、全てのネットワークユーザのデータトラフィックには同一の優先度が与えられてきた。しかしながら、保証されたサービス品質に対する弁済を希望するユーザが増大しつつある。よって、相異なったユーザに係るデータトラフィックを弁別することが可能であることへの要求が存在する。

【0005】 第三に、企業はその内部のデータネットワーク（すなわちイントラネット）に対するかなりの投資を行っており、それらのネットワークの利用状況をより詳細にモニタする方法を求めている。この種の利用状況情報は、課金、ネットワークプランニング、及びネットワーク資源の悪用の発生可能性の制御に係る基礎となる。

【0006】 現在のデータネットワークにおけるユーザ

の利用状況に係る一つの問題点は、データネットワークを介して伝達されるデータパケットが当該データパケットを送受信するユーザを識別しない、という点である。その代わり、データパケットは、データパケットが送出元の機械のアドレス（ソースアドレス）及びデータパケットの送出先の機械のアドレス（デスティネーションアドレス）を識別する。公知のインターネットプロトコル（IP）に従って機能させられているネットワークにおいては、これらのアドレスは IP アドレスと呼称され

る。IP アドレスは、一般に、種々の理由から特定のユーザに対してマッチングされることは不可能である。この種の理由の一つは、IP アドレスがしばしば動的に割り当てられ、その結果、特定の機械のアドレスがその機械がデータネットワークに登録されるたび毎に変化する可能性がある、というものである。別の問題は、機械が固定 IP アドレスを有している場合においても、あらゆる時刻において、複数のユーザがデータネットワークへのアクセス目的で同一機械を用いる、ということである。

【0007】

【発明が解決しようとする課題】 ユーザ固有の利用状況に基づく情報を提供するために種々の試みがなされている。それらの試みの一つは RADIUS プロトコルであり、これは認証であって、RADIUS サーバとダイヤルインネットワークアクセスサーバとの間での通信に利用して用いられる認証課金プロトコルである。加入者が、認証に RADIUS プロトコルを用いるネットワークアクセスサーバにダイヤルする際、サービスプロバイダはそのダイヤルインセッションの間のその特定のユーザによる利用状況を追跡することが可能となる。ユーザは RADIUS サーバによって認証されたため、サーバはユーザの識別及びそのダイヤルアップセッションにおいてそのユーザ宛に割り当てられた IP アドレスの双方を知っていることになる。さらに、ユーザがネットワークアクセスサーバを介してデータネットワークに接続されているため、そのユーザに係る全てのデータトラフィックはネットワークアクセスサーバを経由しなければならない。よって、利用可能なデータを組み合わせることによって、サービスプロバイダはユーザ固有の利用状況データを追跡することが可能となる。それ以前の技法に関する明らかな改善はあるものの、RADIUS プロトコルはサービスプロバイダのシステムに対してダイヤルアップする加入者に係るそのダイヤルアップセッションの間だけのユーザ利用状況を追跡することができるのみである。RADIUS プロトコルに関するさらなる情報は、例えば、C. Rigney 氏による“リモート認証ダイヤルインユーザサービス（RADIUS）”（IETF ネットワークワーキンググループの RFC 2138、1997 年 4 月）；及び、C. Rigney 氏による“RADIUS 課金”（IETF ネットワークワーキンググループの RFC 2

139、1997年4月)より得られる。

【0008】用いられている他の技法は、種々のネットワークロケーションにおいて収集されたデータの相関である。現在では、多くのネットワークノードは、監査、セキュリティ、及び課金などの目的のために利用状況ログを記録する。例えば、シスコシステムズ社(Cisco Systems, Inc.)より市販されているNetFlowという製品は、ルータ及びスイッチなどのネットワークノードにおける利用状況ログを記録するソフトウェアコンポーネントである。NetFlowは、IPアドレス間のデータパケットフローを記録し、さらに、データパケットがノードによって処理される時間間隔も記録する。同様に、Microsoft NTドメインサーバやRADIUSサーバなどのネットワーク認証デバイスは、ユーザによるネットワークに対するログオン及びログオフに係る認証ログを生成する。これらの認証ログは、ユーザID、セッションの間にユーザIDに対して割り当てられたIPアドレス、及びユーザがシステムに対してログオン及びログオフした時刻を含んでいる。利用状況ログ及び認証ログが集中的に収集される場合には、これらログに含まれる情報の相関を調べることによって、ユーザに係る利用状況を再生成することが可能である。しかしながら、この技法にはいくつかの欠点が存在する。第一に、データが複数の異種ソースより収集されなければならないため、データ収集が複雑である。第二に、双方のログシステムの同期が取られていない場合には、利用状況を特定のユーザに関連付けることが困難あるいは不可能である。第三に、同一のネットワークトラフィックに係る複数の利用状況記録が収集される可能性があつて、利用状況の二重測定になる可能性がある。

【0009】インターネット課金に係る技法は、R. Edell、N. McKeown、及びP. Varaiyaによる“TCPに係るユーザ課金及び価格”という表題の論文(IEEE Journal on Selected Area in Communications、第13巻第7号、1995年9月)に記載されている。記載されている技法は、接続指向インターネットトラフィックに係るユーザの利用状況を測定する。接続指向トラフィックとは、あらゆるデータトラフィックが送出される前に、二台の機械の間の接続が設定されなければならないことを意味している。ゲートウェイは、接続設定要求を認識すると、当該接続に係るユーザを識別するため、その接続を介したトラフィックを識別されたユーザに関連付けることが可能になる。この方式の一つの問題点は、ゲートウェイがユーザの認識を指向する間、接続設定が遅延させられることである。この方式に係る別の問題は、この方式が接続指向通信(例えば、TCPプロトコル)に関してのみ有効であるということである。この方式は、接続なし通信(例えば、UDPプロトコル)に関しては機能しない。

【0010】よって、データネットワークの利用状況を

特定のユーザに関連付ける、より改善された技法に関する要求が存在する。

【0011】

【課題を解決するための手段】本発明は、ネットワークトラフィックを特定のユーザに対して実質的にリアルタイムで関連付ける方法を提供する。

【0012】本発明に従って、ネットワークモニタリングノードは、ネットワーク認証ソースから認証データを受信する。認証データは、通常、認証済みユーザの識別及び当該ユーザに係る現時点でのネットワークアドレスを含んでいる。この認証データはモニタリングノードに蓄積される。その後、ネットワークアドレスを含むデータパケットの受信にตอบสนองして、モニタリングノードは、データパケットのネットワークアドレスをストアされたユーザのネットワークアドレスと比較することによって、ユーザをデータパケットに関連付ける。モニタリングノードは、ユーザの利用状況データを生成し、ユーザの利用状況データをデータベースに供給する。この利用状況データは、与えられたユーザに関して集積される。

【0013】本発明の一実施例に従って、ネットワーク認証ソースのうちの少なくとも一つが、ネットワークに接続するユーザを認証するネットワーク認証サーバとなる。ネットワーク認証サーバは、ユーザの認証に即時にตอบสนองして、認証データを生成してモニタリングノード宛に送出する。本発明の別の実施例においては、ネットワーク認証ソースのうちの少なくとも一つが、複数の同時ユーザを有する共用コンピュータである。共用コンピュータは、ユーザによるデータ転送の開始に即時にตอบสนองしてユーザ認証データを生成してモニタリングノード宛に送出するコンピュータプログラムコードを有するソケットライブラリを含むように配置されている。

【0014】本発明の一実施例に従って、モニタリングノードは、受信されたデータパケットに係るサービス、すなわちサービス品質の決定をも行なうことが可能である。

【0015】有利なことには、本発明は、ユーザレベルにおいてリアルタイムサービスを提供する目的で、種々のネットワークアプリケーションと共に用いられうる。このようなサービスは、従来技術においてはユーザレベルで提供され得なかったものである。例えば、本発明は、ユーザレベル課金システム、ファイアウォール、ゲートウェイ、プリペイドサービス、ネットワークポリシー強制、及びサービス品質モニタリングなどを実装する目的で用いられうる。

【0016】本発明に係る上記及びその他の利点は、以下の発明の詳細な説明及び添付図面を参照することによって明らかになる。

【0017】

【発明の実施の形態】図1は、本発明がネットワークにおいて実装される場合の様式で配置されたデータネット

ワークのコンポーネントを示す模式図である。図1に示された実施例においては、モニタリングノード130が、ネットワークリンク132内に、ネットワークリンク132を介して伝達されるネットワークトラフィックをモニタするように配置されている。モニタリングノード130は、モニタされたネットワークトラフィックを特定のユーザに対して実質的にリアルタイムで関連付ける。この、ネットワークトラフィックの特定のユーザに対する関連付けは、モニタリングノード130内にストアされた認証データを参照することによって実行される。

【0018】認証データは、ネットワーク認証ソースからモニタリングノード130によって受信される。四つの認証ソース例110、112、114、116が図1に示されている。認証ソース110、112、及び114は、データネットワークへのアクセスあるいはデータネットワーク上のアクセス可能な資源へのアクセスを得ることを望むユーザを認証する目的で用いられる。NTドメインサーバは、マイクロソフトWindows NTのローカルエリアネットワーク上にログオンしているユーザを認証する。ダイヤルアップサーバ112は、ダイヤルアップサービスプロバイダにログインするユーザを認証する。ダイヤルアップサーバ112は、前述されているように、RADIUSサーバを含むことも可能である。共用システム114は、例えば、複数のユーザが同時にログオンすることが可能な共用UNIX（登録商標）システムなどの共用コンピュータシステムを表わしている。これらのシステムは、通常、ユーザがユーザID及びパスワードの入力を行なうことを要求することによってユーザを認証する。認証データをモニタリングノード130に供給する目的で、認証ソース110、112、114は、さらに、それぞれモニタ120、122、124を有している。これらのモニタは、ユーザの認証に際して認証データをモニタリングノード130宛に送出する追加された機能を実現するソフトウェアモジュールを表わしている。

【0019】認証サーバ110及び112に関して、認証データはモニタリングノード130宛に、認証サーバ110あるいは112にいずれかによるユーザの認証に即時に応答して供給される。よって、ユーザの認証がなされると、当該ユーザに係る認証データがモニタリングノード130宛に即時に送出される。もちろん、認証サーバ110、112、モニタ120、122、及びモニタリングノード130との間の通信リンクの設計に起因する通常の処理及び伝播遅延に依る、モニタリングノード130による情報受信の遅延は存在することに留意されたい。しかしながら、そのような遅延は副次的なものであり、認証データは、ユーザの認証に引き続いて即時的にモニタリングノード宛に送出されて受信されることが企図されている。共用システム114に関しては、認

証データはモニタ124によって、ユーザによるデータ転送の開始に即時に応答して、モニタリングノード130宛に送出される。共用システム114及びモニタ120、122、124の詳細に係る側面については、後に詳細に記述される。

【0020】設置されている認証ノード116は、データネットワークへのアクセスを指向するユーザを認証しないが、その代わりに、モニタリングノード130に対するアクセスを有する管理機能を代表している。設置されている認証ノード116は、モニタリングノード130宛の認証データの直接供給を可能にする。後の記述より明らかになるように、認証データの直接供給は、例えば一群のユーザに係る認証データの提供の際などに有用である。

【0021】モニタリングノード130は、ネットワークトラフィックを特定のユーザに関連付ける際、その情報をデータベース140宛に供給する。データベース140は、情報をストアし、これらのデータをさらに相關付ける目的で、ある種のデータ処理を実行する。その後、データベース140は、データをネットワークアプリケーションに対して供給する。あるいは、モニタリングノード130は、ネットワークアプリケーションに対して直接データを供給する。ネットワークアプリケーション例は後に詳細に記述される。

【0022】モニタリングノード130の機能ブロック図が図2に示されている。モニタリングノード130は、二つのネットワークインターフェース202、206を有している。ネットワークインターフェースの個々のタイプは、モニタされるネットワークのタイプ（例えば、イーサネット（登録商標））に依存する。ネットワークインターフェースはネットワークドライバ204に接続されている。データパケットがいずれかのネットワークインターフェース202、206において受信されると、ネットワークドライバ204は、そのデータパケットをどのように取り扱うかを決定する。データパケットは、以下の三つの一般的なカテゴリに分類される。第一に、データパケットは、モニタリングノード130以外のネットワークノード宛のデータパケットである可能性がある。この場合には、ネットワークドライバ204はそのデータパケットを宛先アドレス宛に伝達する目的で他方のネットワークインターフェースに転送する。ネットワークドライバ204は、特定のユーザ及びサービスをデータパケットと関連付ける目的でモニタリングデータ214をアクセスする。より詳細に述べれば、ネットワークドライバ204は、特定のユーザ及びサービスをデータパケットと関連付ける目的で、認証データ218及びサービステーブル220をアクセスする。それが成功すると、ネットワークドライバ204は利用状況データ216を適切に更新する。特定のユーザ及びサービスのデータパケットとの関連付け及び利用状況データ

216の更新に関しては、後に詳細に議論される。データパケットの第二のカテゴリは、モニタリング機能の実行に用いられる目的でのモニタリングノード130宛のデータパケットである。前述されているように、認証ソース110、112、114、116（図1）は、認証データをモニタリングノード130宛に送出する。この認証データは、ネットワークを介して送出され、ネットワークノード130によって、ネットワークインターフェース202、206のうちのいずれかにおいて受信される。ネットワークドライバ204は、認証ソースからの認証データの受信を認識し、認証データ218を適切に更新する。

【0023】モニタリングノード130は、ネットワークトラフィックモニタリングアプリケーション以外の他のネットワークアプリケーションに対するホストとして機能しうることに留意されたい。そのような実施例においては、第三のカテゴリに属するデータパケットが存在し、それらは、モニタリングノード130宛ではあるが、そのような他のネットワークアプリケーションに係るものである。ネットワークドライバ204はこれらのデータパケットを認識し、それら処理目的でIPプロトコルスタック208宛に転送する。

【0024】ネットワークノード130は、モニタリングノード130のモニタリング機能のうちのいくつかを制御するコントローラ222も含んでいる。コントローラ222は、他のネットワークエレメントとの通信を可能にするIPプロトコルスタック208との通信を行なう。コントローラ222の機能の一つは、サービステーブル22Qと、他の認証ノード216などの外部ネットワークノードから得られた認証データ218の管理を制御することである。コントローラ222は、さらに、モニタリングノード130からデータベース140への利用状況データ216の転送をも制御する。ここで示されている実施例においては、コントローラ222は、IPプロトコルスタック208を介しネットワークインターフェース202、206のうちのいずれかを通じてデータベース140と通信する。別の実施例においては、コントローラ222は、専用（図示せず）のI/Oポートを介してデータベース140と通信する。

【0025】モニタリングノード130は、適切にコンフィギュアされてプログラミングされたデジタルコンピュータを用いて実装されうる。よって、本明細書において記述されるモニタリングノードの機能は、ストアされたコンピュータプログラムコードを実行するプロセッサの制御下で実行される。プログラムされたデジタルコンピュータは当業者には公知であり、プログラムされたデジタルコンピュータを用いてモニタリングノード130を実装するために必要となるプロセッサ、メモリなどの公知のコンポーネントは図2には示されていない。当業者は、本明細書における記述が与えられれば、モニタリ

ングノードを容易に実装することが可能である。ネットワークインターフェース202、206は、コンピュータの一部でありうるハードウェアデバイスを表わしている。ネットワークドライバ204、IPプロトコルスタック208、及びコントローラ222は、本明細書に記載されている機能を実装するために用いられるソフトウェアモジュールを表わしている。

【0026】図2に示されているように、IPプロトコルスタック208、ネットワークドライバ204、及びモニタリングデータ214は、コンピュータのオペレーティングシステムカーネル空間226内のメモリに配置されている。カーネル空間226は、オペレーティングシステムカーネルによってのみアクセス可能な部分のコンピュータメモリを表わしている。コントローラ222は、ユーザ空間224内に位置している。ユーザ空間224は、ユーザソフトウェアモジュールによってアクセス可能な部分のコンピュータメモリを表わしている。一般に、カーネル空間226内でなされる処理は、ユーザ空間224内でなされる処理よりも高速である。図2に示されたアーキテクチャは、大部分のデータパケット処理プロセスがカーネル空間226内でなされるために有利である。さらに、このアーキテクチャは、データパケットをカーネル空間226からユーザ空間に移動するという付加的なコストを回避している。コントローラ222は、その処理時間が重要になるような操作を行なわないために、ユーザ空間224に適切に配置されている。このような本発明に係るモニタリングノード機能の有利な設計により、受信したデータパケットの特定のユーザへの関連付けが実質的にリアルタイムでサポートされる。別の実施例においては、データパケット処理機能のうちのある部分あるいはその全てがユーザ空間224において実行される。このことによって付加的なオーバーヘッドが導入されるが、ソフトウェア開発及び管理が簡潔化される。

【0027】モニタリングデータ214は、図3から図5を参照してより詳細に記述される。図3は、ストアされた利用状況データ216のフォーマットを示しており、それは、モニタリングノード130によってその動作の間に収集されたモニタリング情報を含んでいる。利用状況データ216は、図3に示された形式の記録を含んでいる。ユーザフィールド302はデータパケットに関連付けられた特定のユーザを識別し、s r v cフィールド304は特定のユーザによって用いられるサービスを識別する。これらの記録における残りの部分のデータは、ユーザフィールド302及びサービスフィールド304に基づいて集積されたものである。よって、特定のサービスを用いる特定のユーザに関しては、単一の記録が存在して、残りのフィールドはモニタリングが継続されるに連れて集積される。バイト数フィールド306は転送されたバイト数を含んでいる。パケット数フィール

ド 308 は転送されたパケット数を含んでいる。フロー数フィールド 310 はフロー数を含んでいる。src-IP フィールド 312 はデータパケットのソース IP アドレスを含んでいる。dst-IP フィールド 314 はデータパケットのデスティネーション IP アドレスを含んでいる。src-port フィールド 316 はデータパケットのソースポートを含んでいる。dst-port フィールド 318 はデータパケットのデスティネーションアドレスを含んでいる。後ろ側の四つのフィールド 312、314、316、318 はオプションであり、相異なったユーザ、サービス、あるいはホストに関して管理される場合もあり、管理されない場合もある。これらのフィールドが管理されない場合には、性能が向上する。しかしながら、例えば、特定のユーザによる利用状況を詳しく監査する目的などのように、より詳細な情報を管理することが望ましい場合も存在する。

【0028】多くのコンピューティング環境においては、複数の認証ドメインが共存している。例えば、単一のローカルエリアネットワークは、NT ドメイン認証及び UNIX ドメイン認証の双方をサポートしうる。さらに、ダイヤルアップ接続に関しては、リモートアクセス認証が用いられうる。このことによって、単一のユーザが複数のドメインに亘って複数のユーザ名を有するという問題が生ずる。従って、同一のユーザ名が複数の認証ドメインにおいて、相異なったユーザに対して割り当てられる可能性がある。この問題を処理する目的で、利用状況データ記録のユーザフィールド 302 は、さらに三つのフィールドに分割される。ドメインフィールド 320 は認証ドメインを識別する。認証ドメインが明示的に知られていない場合、ドメイン名を割り当てる一つの技法は、認証を実行しているシステムの IP アドレス（例えば、NT ドメインサーバの IP アドレス）あるいは認証を実行している機械に係るプロキシの IP アドレスを用いることである。タイプフィールド 322 は実行された認証のタイプである。例えば、このタイプは、認証サーバのタイプに依存して、“UNIX”、“NT”、あるいは“RADIUS”として識別される。uid フィールド 324 は、その特定のドメインに係るユーザ識別子である。ドメインフィールド 320、タイプフィールド 322、及び uid フィールド 324 をユーザ識別目的で利用することにより、利用状況データの監査も可能になる。この種の監査には、モニタが利用状況を特定のユーザに関してどのように関連付けたかに係る事後の決定が含まれる。

【0029】ネットワーク利用状況を特定のユーザに関連付けるのみならず、モニタリングノード 130 は、ユーザによって利用されているサービスを識別する機能をも有している。src フィールド 304 は、さらに三つのフィールドに分割されている。サービスタイプフィールド 326 はサービスタイプを識別する。本発明の一

実施例においては、サービスタイプフィールド 326 は、ETHER、IP、TCP、あるいは UDP を含む。IP アドレスフィールド 328 は IP アドレスを含んでいる。サービスフィールド 330 は、サービスタイプフィールド 326 によって規定されたサービスクラス内の特定のサービスを識別するコンテキストセンシティブコードを含んでいる。本発明の一実施例において、サービスタイプフィールド 326 が ETHER である場合には、サービスフィールド 330 はイーサネットプロトコル番号を有している。サービスタイプフィールド 326 が IP である場合には、サービスフィールド 330 は標準的な IP プロトコル番号（例えば、IP/ICMP に関しては 1、IP/TCP に関しては 6、及び、IP/UDP に関しては 17）を有している。サービスタイプフィールド 326 が TCP あるいは UDP の場合には、サービスフィールド 330 はサービスのポート番号（HTTP の場合には、サービスタイプフィールド 326 は TCP を有しており、サービスフィールド 330 は 80 を有している；これは、HTTP サービスに関する標準的なポートである）を有している。

【0030】図 4 は、ストアされた認証データ 218 記録のフォーマットを示している。これらの記録におけるデータは、認証ソースから受信され、モニタされたネットワークトラフィックを特定のユーザに関連付ける目的で利用される。認証データ 218 は、特定のユーザに IP アドレス、プロトコル、及びポートを関連付ける記録を有している。それらのフィールドに関しては以下に概説されるが、これらのフィールドの、特定のユーザに対してネットワークトラフィックを関連付ける目的での利用に関しては、後に詳述される。IP-addr フィールド 402 は IP アドレスを有しており、マスクフィールド 404 はマスクとして用いられる 32 ビット数を有しており、proto フィールド 406 は IP プロトコル番号（例えば、UDP（17）あるいは TCP（6））を有しており、ポートフィールド 408 はポートの識別を有しており、及びユーザフィールド 410 は特定のユーザを識別する。ユーザフィールド 410 は、さらに、ドメインフィールド 412、タイプフィールド 414、及び uid フィールド 416 に分割されている。フィールド 412、414、及び 416 は、図 3 に関連して上述されているフィールド 320、322、及び 324 と同一である。

【0031】図 5 は、サービステーブル 220 の記録のフォーマットを示している。これは、特定のユーザの利用状況に関連付けられたサービスを識別する目的で用いられる。そのフィールドに関しては以下に概説されるが、ネットワークトラフィックを特定のユーザに関して関連付ける目的でのこれらのフィールドの利用に関しては後に詳述され、その時点でこれらのフィールドの利用が明確になる。IP-addr フィールド 502、マス



クフィールド 504、及び protocol フィールド 506 は、図 4 に関連して上述されたフィールド 402、404、及び 406 と同一である。ポート範囲フィールド 508 はポート識別の範囲を有している。

【0032】図 6 は、IP プロトコルに従った TCP データパケットのフォーマットを示している。IP プロトコルは公知であり、本発明に関連しているフィールドのみが記述される。データパケット 600 は、IP ヘッダ 602、TCP ヘッダ 604 及び TCP データ 606 を含んでいる。IP ヘッダ 602 は、プロトコル 608、ソース IP アドレス 610 及びデスティネーション IP アドレス 612 を含む複数のフィールドより構成されている。TCP ヘッダ 604 も、ソースポート 614 及びデスティネーションポート 616 を含む複数のフィールドより構成されている。図 6 に示された TCP データパケットは、本発明に従って処理されるデータパケットの一例である。しかしながら、本発明は TCP パケットの処理に限定されているわけではない。当業者には、本発明が他のプロトコルに従って送信されるデータパケットの処理を行ないということが明白である。例えば、それらのプロトコルにはイーサネット、IP、UDP、RPC、NFS（登録商標）、SMTP などがあるが、それらに限定されている訳ではない。

【0033】本発明に従ったモニタリングノード 130 の動作が図 7 から図 9 の流れ図を参照して以下に記述される。流れ図に示された段階は、ストアされたコンピュータプログラムコードに従って、モニタリングノード 130 のプロセッサによって実行される。図 7 は、データパケットを受信した際にモニタリングノード 130 によって実行される段階を示している。段階 702 では、データパケットがモニタリングノード 130 によって受信される。このパケットは、モニタリングノード 130 以外のネットワークノードに宛てたものであって、モニタリングノード 130 がそのデータパケットへの特定のユーザ及びサービスの関連づけを試行している、ということが仮定されている。段階 704 では、モニタリングノード 130 は、受信したデータパケットが、特別の処理が必要とされるある種の既知のプロトコルに従ってデータを伝達しているデータパケットであるか否かを決定する。データパケットの特別な処理に関しては後述される。データパケットが特別の処理を必要とするデータを伝達していない場合には、制御が段階 706 へ進み、そのデータパケットのソースであるユーザの識別に係る試行がなされる。ユーザ識別段階 706 は、さらに、図 8 に示された流れ図に関連して詳述される段階も含んでいる。ユーザが識別されない場合には、段階 710 において、データパケットの宛先であるユーザの識別に係る試行がなされる。この段階 710 は段階 706 と同一であり、後に図 8 に関連して詳述される。段階 712 においては、段階 710 でユーザが識別されたか否かが決定さ

れる。ユーザが段階 708 あるいは段階 712 において識別された場合には、段階 714 において、データパケットに関連付けられたサービスの識別が試行される。段階 712 においてユーザが識別されなかった場合には、この方法は段階 718 で終了する。サービス識別段階 714 は、後に図 9 の流れ図に関連して詳述される段階を含んでいる。段階 716 においては、利用状況データ 216（図 2）が段階 706 あるいは 710 において識別されたユーザ、及びサービス（段階 714 で識別された場合）に従って更新される。

【0034】段階 704 では、受信されたパケットが特別の処理を必要とするか否かが決定される。ある種のプロトコルは、データを、当該データを送出するユーザが当該データを送出するように要求されたユーザではない、という様式で送付する。例えば、UNIX システム上のネットワークファイルシステム（NFS）プロトコル要求は、通常、システム管理者によって所有されるプロセスによって開始され、データを要求しているユーザによって所有されるプロセスからではない。同様に、e メール（電子メール）も、メールを送信するユーザによってではなく、メーラーデーモンによって所有されるプロセスによってフォワードされる。別の例は、ウェブ（web）ホストサービスを提供するウェブサーバである。ウェブサーバはデータを伝送するが、考慮されべきユーザはその内容が転送される宛先のユーザである。これら、また他の特別な場合において、アプリケーションに特有の技法が、ネットワークを介したデータの発信あるいは受信を行なっているユーザを識別する目的で用いられなければならない。最も一般的には、これらの技法には、パケットヘッダのみならずそのパケットの内容に対する調査が含まれる。よって、段階 704 におけるテストが yes である場合には、段階 720 において、特別の処理アルゴリズムがユーザ識別を決定する目的でデータパケットに対して適用される。標準的ではないプロトコルの各々は、それぞれに係る特別の処理アルゴリズムを有している。データ通信の当業者は、所定のプロトコルに対するその種のアルゴリズムを容易に実装可能である。

【0035】図 3 を参照して、利用状況データ 216 における記録は、新たなユーザ識別及びサービス識別を（それぞれ存在する場合には）反映するように更新される。識別されたユーザ及びサービス対を含む利用状況記録が既に存在する場合には、バイト数フィールド 306、パケット数フィールド 308 及びフロー数フィールド 310 が、その新たなデータパケットを反映するように更新される。識別されたユーザ及びサービス対を含む利用状況データ記録が存在していない場合には、適切な情報を含む新たな記録が生成される。このようにしてユーザデータ 216 を更新することにより、それぞれ独自のユーザ／サービス対の各々に対して単一の記録が生成

される。

【0036】図8は、特定のデータパケットに係るユーザを識別する段階706、710をより詳細に示した流れ図である。段階706の結果として図8に示された段階が実行される場合は、IPアドレスは受信されたデータパケットのソースIPアドレス610（図6）である。段階710の結果として図8に示された段階が実行される場合は、IPアドレスは受信されたデータパケットのデスティネーションIPアドレス612である。段階802では、認証データ記録218に対する指数

(i) が1にセットされる。図8における記述で用いられる“フィールド名”[i]という表現は、認証データ218におけるi番目の記録における“フィールド名”を有するフィールドの値を表わしている。段階804では、データパケットのIPアドレスにマスク[i]が適用される。二つの値を比較する前にマスクを適用することは公知の技法である。ここでは、マスクが、データパケットのIPアドレスの範囲が単一の認証データ記録のIP-addr（フィールド402）に一致するか否かを検出する目的で用いられる。このことは、例えば、特定のサブネットに属するユーザを識別するような課金アプリケーションにおいて有用である。

【0037】段階806では、マスクされたデータパケットのIPアドレスがIP-addr[i]と比較される。一致がない場合には、段階808において、認証データ218内に別の記録が存在するか否かが決定される。別の記録が存在しない場合には一致はなく、この方法は段階830で終了する。さらなる記録が存在する場合には、段階810において指数iが1だけ増加させられ、制御は804へ戻る。マスクされたデータパケットのIPアドレスがIP-addr[i]と一致する場合には、段階806でのテストの結果はYESであって、段階812において、proto[i]が規定されているか否かが決定される。すなわち、段階812は、i番目の認証記録におけるprotoフィールド406が値を有しているか否かを決定する。有していない場合には一致はなく、この方法は段階830で終了する。段階812のテスト結果がYESである場合には、段階814で、受信されたデータパケットのプロトコル（フィールド608）がproto[i]と一致するか否かが決定される。段階814のテスト結果がNOである場合には、i番目の認証記録は受信されたデータパケットと一致せず、制御は段階808へ移る。段階814のテスト結果がYESである場合には、段階816において、proto[i]がTCPあるいはUDPであるか否かが決定される。段階816のテスト結果がNOである場合には、一致が存在し、この方法は段階830で終了する。段階816でのテスト結果がYESである場合には、段階818において、port[i]が規定されているか否かが決定される。規定されていない場合には、

一致が存在し、この方法は段階830で終了する。段階818でのテスト結果がYESである場合には、段階820において、受信されたデータパケットのポート（図8に示された方法が図7の段階706から実行された場合にはソースポートフィールド614であり、図8に示された方法が図7の段階710から実行された場合にはデスティネーションポートフィールド616である）がport[i]と一致するか否かが調べられる。段階820のテスト結果がNOである場合には、i番目の認証記録は受信されたデータパケットと一致せず、処理は段階808へ戻る。段階820のテスト結果がYESである場合には、一致が存在し、この方法は段階830で終了する。

【0038】図9は、特定のデータパケットに係るサービスを識別する段階714（図7）をより詳細に示した流れ図である。図9に示された段階は、まず、受信されたデータパケットをサービスに関連付ける目的で、受信されたデータパケット600のソースIPアドレスフィールド610及びソースポートフィールド614を用いることによって実行される。ソースIPアドレスフィールド610及びソースポートフィールド614を用いてサービスが見出さない場合には、図9の段階は、受信されたデータパケットをサービスに関連付ける目的で、受信されたデータパケット600のデスティネーションIPアドレスフィールド612及びデスティネーションポートフィールド616を用いることによって実行される。

【0039】段階902では、サービステーブル220に係る指数(i)が1にセットされる。図9の記述に関しては、フィールド名[i]という表現は、サービステーブル220におけるi番目の記録のフィールド名を有するフィールドの値を示している。段階904においては、データパケットのIPアドレスがマスク[i]によってマスクされる。段階906では、マスクされたデータパケットのIPアドレスが、IP-addr[i]と比較される。一致がない場合には、段階908において、サービステーブル220にさらに記録が存在しているか否かが決定される。記録が存在しない場合には、そのサービスは未知であってこの方法は段階922で終了する。さらに記録が存在する場合には、段階910において指数iが1だけ増加させられて、制御が段階904に戻る。マスクされたデータパケットのIPアドレスがIP-addr[i]と一致する場合には、段階906でのテスト結果がYESであり、段階911においてproto[i]が規定されているか否かが決定される。すなわち、段階911は、i番目のサービステーブル記録におけるprotoフィールドが値を有しているか否かを決定する。値を有していない場合には、一致が存在して制御は段階916へ進む。段階911のテスト結果がYESである場合には、段階912において、受信さ

れたデータパケットのプロトコル（フィールド608）が `proto[i]` と一致するか否かが決定される。段階912におけるテスト結果がNOである場合には、i番目のサービステーブル記録は受信されたデータパケットと一致せず、制御は段階908へ進む。段階912におけるテスト結果がYESである場合には、段階913において、`port-range[i]` が規定されているか否かが決定される。すなわち、段階913は、i番目のサービステーブル記録におけるポート範囲フィールド508が値を有しているか否かを決定する。値を有していない場合には、一致が存在して制御は段階916へ進む。段階913におけるテスト結果がYESである場合には、段階914において、受信されたデータパケットのポートが `port-range[i]` によって規定された範囲内にあるか否かが決定される。段階914のテスト結果がNOである場合には、i番目のサービステーブル記録は受信されたデータパケットと一致せず、制御は段階908へ進む。段階914におけるテスト結果がYESである場合には、段階916に示されているようにサービスが識別されたことになる。よって、利用状況データ216が段階716において更新される際には、サービスタイプフィールド326には受信されたデータパケットのプロトコル（フィールド608）の値が割り当てられ、IP-addressフィールド328にはマスクされたデータパケットのIPアドレス（段階904で決定されたもの）が割り当てられ、サービスフィールド330にはデータパケットのポートの値が割り当てられる。この方法は段階922で終了する。

【0040】以下、モニタ120、122、及び124の実装の詳細な議論が記述される。

【0041】ある実施例においては、モニタ120及び122は、それぞれ認証サーバ110及び112の認証ログをモニタする。認証ログに対して新たな認証データが生成されると、関連しているモニタがその情報をモニタリングノード130宛に即時転送する。

【0042】NTドメインサーバ110に係るモニタ120の別の実施例においては、モニタ120は、ネットワーククリティカルオペレーション（例えば、ログオン及びログオフなど）の性能に係る通知を自動的に受信するように登録されたNTサービスとして実装される。この種の通知を受信すると、モニタ120は適切な認証データをモニタリングノード130宛に即時送信する。

【0043】ダイヤルアップサーバ112に関しては、ある種のダイヤルアップサーバはNTドメインサーバ110に関連して上述されているものと同様の通知機構を実現し、これらは認証モニタ122を実装する目的で用いられる。加えて、ダイヤルアップサーバ112がRADIUSサーバとして実装される場合には、モニタ122はRADIUSクライアントと実際のRADIUSサーバとの間のプロキシRADIUSサーバとして実装さ

れる。この実装においては、プロキシはクライアントとRADIUSサーバとの間の全RADIUS要求及び応答を転送する。加えて、副次的な効果として、プロキシはユーザ認証に即時に回答してモニタリングノード130宛に認証データを生成して送出する。

【0044】以下、共用コンピュータシステム114に係るモニタ124の一つの有利な実施例が記述される。この実施例においては、UNIXオペレーティングシステムの共有オブジェクトアーキテクチャ及び動的リンク機能を用いられている。共有ライブラリは、ワールドワイドウェブサーバ及びブラウザ、及びFTPサーバ及びクライアントなどの標準的なネットワークアプリケーションに対して、オペレーティングシステムによって自動的に動的にリンクされる。この実施例に従って、既存の共有ソケットライブラリ（通常、`libsocket.so` と呼称されるもの）が、新たなソケットライブラリによって置換される。この新たなライブラリは、元のソケットライブラリと同一のオペレーションの全てを含んでおり、さらに、ネットワークオペレーションの少なくともいくつかに関して、付加的なラッパーコードが挿入されている。この有利な実施例において、新たなコードでラップされている機能には、`bind`、`connect`、`sendmsg`、`sendto`、`recvfrom`、及び`recvmsg`が含まれる。これらの機能が実行される際には、付加されたラッパーコードは、認証データをモニタリングノード130宛に送出する認証メッセージを生成する。認証情報は、通常、共有コンピュータシステム114のIPアドレス、特定のユーザのプロセスが通信しているTCP及びUDPポート、及び当該ユーザの識別を含んでいる。よって、この状況では、認証データは、ユーザによるデータ転送の開始に即時に回答して送出される。

【0045】モニタ120、122、124に係る上記記述は、モニタがどのようにして認証データを生成するかに係るものである。ひとたび生成されると、認証データはモニタリングノード130宛に送出される。図1においては、モニタリングノード130が認証ソース110、112、114、116に接続されているように示されているが、これは論理的な接続であって、実際、認証ソース110、112、114、116からモニタリングノード130宛に送出される認証データは、単一あるいは複数のサブネットワークを通過することを求められる場合があることに留意されたい。加えて、認証データは、データネットワークの複数のサブネットワークにおける複数のモニタリングノード宛に送出される場合もある。以下、認証データをモニタリングノード宛に送出するための二つの方法が記述される。

【0046】認証サーバ110及び112は、ブロードキャスト認証と呼称される方法を用いており、認証データは認証サーバからモニタリングノード宛の特別なメッ

セージにおける認証データとして送出される。これらのメッセージは、モニタリングノードが位置しているサブネットワークにおけるブロードキャストアドレス宛に送出される。これらの特別のメッセージは、モニタリングノードによって受信されて処理される。モニタリングノードが位置しているサブネットワークのブロードキャストアドレスは、認証サーバ 110、112 に与えられている。

【0047】共有コンピュータシステムよりなる認証ソース 114 は、認証データをモニタリングノード宛に送出するための二つの技法のうちの一を用いる。前述されているように、共有コンピュータシステム 114 のモニタ 124 は、共有システム 114 のユーザによるデータ転送の開始に際して認証データを送出する。ユーザが接続指向送信を開始する際には、前述されたブロードキャスト認証技法が用いられる。認証ソース 114 によってブロードキャスト認証が用いられる場合には、ブロードキャストアドレスはその機械が接続されているサブネットワークのブロードキャストアドレスである。そのサブネットワーク宛に送出することによって、全ての介在するモニタリングノードが認証データを含む特別のメッセージを受信することが可能になる。ユーザが接続無し送信を開始する場合には、共有システム 114 は、タグ認証と呼称される別の方法を利用する。この方法に従って、全ての発信メッセージには付加的な認証データがタグとして付加される。発信メッセージにタグを付加する一つの方法は、認証データを IP パケットヘッダのオプションフィールドに挿入することである。この技法は、発信メッセージにのみ作用する（なぜなら、着信メッセージにはタグが付されえないからである）。接続無し送信における発信メッセージに関しては、前述されたブロードキャスト認証も用いられうることに留意されたい。タグあるいはブロードキャスト認証のいずれを発信データパケットに対して用いるかは、送出されるパケットの予想数に依存する。接続無し送信における着信パケットに関しては、ブロードキャスト認証が用いられなければならない。しかしながら、モニタリングノードは、データパケットを正確に処理することが可能であるためには、データパケットの受信前に認証データのブロードキャストを受信しなければならない。このタイミング問題を取り扱う一つの技法は、モニタリングノードがブロードキャスト認証データを受信するまで、接続無し送信における入力パケットをバッファリングすることである。

【0048】データパケットに係るユーザ及びサービス情報を決定するための上述された方法は、完全な IP 及び関連している場合には TCP あるいは UDP ヘッダが利用可能である場合に用いられる。しかしながら、ある種のネットワークにおいては、大きなメッセージが複数個のより小さいパケットに分断されてしまう。上述されているような、ユーザ及びサービスを決定するために必

要とされるヘッダ情報は、分断されたパケットのうちの最初のもののみにおいて利用可能である。このような状況を取り扱う目的で、第一パケットから決定されたユーザ及びサービス情報は、モニタリングノード 130 内にストアされうる。同一メッセージの残りの部分がモニタリングノード 130 において受信された際に、ストアされたユーザ及びサービス情報がその残りの部分に対しても適用される。IP ヘッダにストアされた分断情報は、モニタリングノード 130 が分断されたパケットをそれ以前に受信されたヘッダから適切なユーザ及びサービス情報に関連付けることを可能にする。

【0049】以上の記述より明らかなように、モニタリングノード 130 は、特定のユーザのネットワークトラフィックに対する関連づけを可能にする。この技法と共に用いられうるネットワークアプリケーションは多数存在する。課金アプリケーションは、ネットワークトラフィック量、日時、及び用いられた特定のサービス等のファクタを含む、特定のユーザによるネットワーク利用状況に基づいて特定のユーザに課金する目的で、データベース 140 にストアされたネットワーク利用状況を利用できる。サービス品質 (QoS) ネットワークアプリケーションも実装可能である。モニタリングノード 130 を用いることにより、特定のユーザによって受容されるサービス品質をモニタすることが可能になる。QoS ネットワークアプリケーションは、QoS サービスが所定のレベル未満に低下した場合にユーザに弁済する目的で用いられることも可能であり、また、QoS の所定のレベルを回復するためにネットワークにおける修正操作を行なう目的でも用いられうる。例えば、IP テレフォニーの双端における二つのモニタリングノードが、通話によって受容されるエンドツーエンドサービス品質を測定する目的で使用されうる。これは、例えば平均あるいは最大レイテンシの観点で測定される。この情報は、種々の料金プランの基礎を構成しうる。ファイアウォールアプリケーションは、特定のソースあるいはデスティネーションユーザに基づくネットワークトラフィックを制限する目的で用いられる。現時点のファイアウォールは、通常、ソースあるいはデスティネーション IP アドレスに基づいてトラフィックを制限する。しかしながら、前述されているように、IP アドレスは特定のユーザを識別しない。上述されたネットワークモニタを用いることにより、ファイアウォールアプリケーションが特定のユーザに基づいてネットワークトラフィックを制限することが可能になる。課金アプリケーション、サービス品質アプリケーション、及びファイアウォールアプリケーションは専用のネットワークノードを用いて実装されうる。あるいは、課金アプリケーション、サービス品質アプリケーション、及びファイアウォールアプリケーションが、スイッチやルータなどの他の目的で用いられうるネットワークノードに組み込まれることも可能で

ある。

【0050】ネットワークトラフィックを特定のユーザに関連付けるデータを用いて他の多くのアプリケーションが実装されうることが当業者には明らかである。例えば、ゲートウェイシステムは、モニタリングノードによって生成された情報を、特定のユーザあるいは特定のユーザクラスから特定のユーザあるいは特定のユーザクラスへのトラフィックを制限する目的で利用することが可能である。ネットワークモニタが特定のユーザによる利用状況をその利用状況が発生する時点で実質的にリアルタイムでモニタするため、プリペイドサービスが実現されうる。さらに、モニタリングノードによって生成されたデータは、時刻、持続時間、あるいは特定のサービス等のファクタに基づいてある種のネットワークポリシーを強要する目的にも用いられうる。

【0051】ある種のネットワークトポロジにおいて、複数のモニタリングノードが存在しうる。結果として、そこをデータパケットが通過するとそれらが複数のモニタリングノードによって処理されてしまうような経路が存在しうる。このことは、ある種のネットワークアプリケーションに関しては問題となりうる。例えば、課金アプリケーションにおいては、同一のデータパケットを複数のモニタリングノードにおいて処理すること正しくない。なぜなら、二重課金になってしまうからである。この多重処理の問題及びそれを解決するための技法は、共願されている“データネットワークにおける単一処理の適用のための方法及びその装置”という表題の米国特許出願第09/316118号（1999年5月20日出願）に記載されている。

【0052】以上の説明は、本発明の一実施例に関するもので、この技術分野の当業者であれば、本発明の種々の変形例が考え得るが、それらはいずれも本発明の技術的範囲に包含される。例えば、図1に示された特定の実施例に関連して記述されているように、モニタリングノード130はネットワークリンク上のブリッジとして機能するスタンドアロンネットワークノードとして示されている。しかしながら、本発明に従ったモニタリングノード130の機能は、例えばスイッチやルータなどの既存のネットワークノード内のモジュールとして実装されうる。さらに、ある実施例においては、本発明は適切にプログラミングされた汎用コンピュータを用いて実装される。あるいは、本発明は、プログラム可能ハードウェアロジックあるいは専用ハードウェアコンポーネントを用いて実装されることも可能である。

#### 【0053】

【発明の効果】以上述べたごとく、本発明によれば、ネットワークトラフィックを特定のユーザに対して実質的にリアルタイムに関連付ける方法が提供される。

#### 【図面の簡単な説明】

【図1】 本発明がネットワークにおいて実装される場

合の様式で配置されたデータネットワークのコンポーネントを示す図。

【図2】 本発明に係るモニタリングノードの機能を示すブロック図。

【図3】 本発明に係る利用状況データレコードのフォーマットを示す模式図。

【図4】 本発明に係る認証データレコードのフォーマットを示す模式図。

【図5】 本発明に係るサービステーブルレコードのフォーマットを示す模式図。

【図6】 IPプロトコルに従ったTCPデータパケットのフォーマットを示す模式図。

【図7】 本発明に従って、データパケットを受信した際にモニタリングノードによって実行される段階を示す流れ図。

【図8】 本発明に従って、特定のデータパケットに係るユーザを識別する目的でモニタリングノードによって実行される段階を示す流れ図。

【図9】 本発明に従って、特定のデータパケットに係るサービスを識別する目的でモニタリングノードによって実行される段階を示す流れ図。

#### 【符号の説明】

110 NTドメインサーバ

112 ダイアルアップサーバ

114 共有システム

116 認証ノード

120、122、124 モニタ

130 モニタリングノード

140 データベース

202 ネットワークインターフェース

204 ネットワークドライバ

206 ネットワークインターフェース

208 IPプロトコルスタック

214 モニタリングノード

216 利用状況データ

218 認証データ

220 サービステーブル

222 コントローラ

224 ユーザ空間

226 カーネル空間

302 ユーザフィールド

304 サービスフィールド

306 バイト数フィールド

308 パケット数フィールド

310 フロー数フィールド

312 ソースIPアドレスフィールド

314 デスティネーションIPアドレスフィールド

316 ソースポートフィールド

318 デスティネーションポートフィールド

320 ドメインフィールド

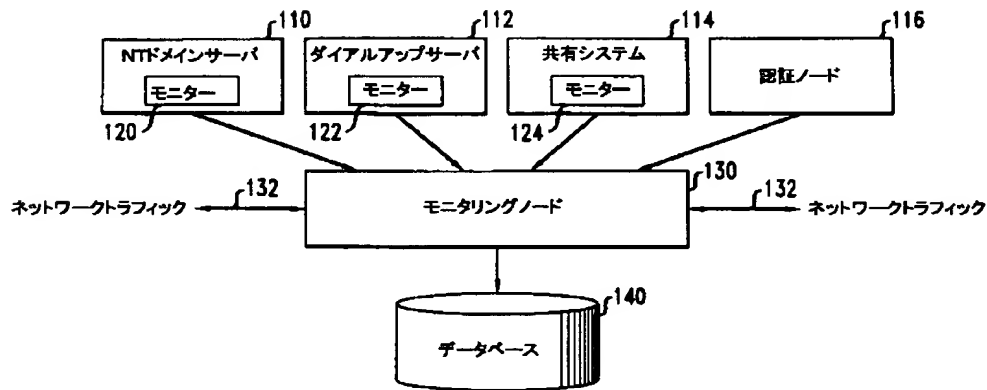
25

26

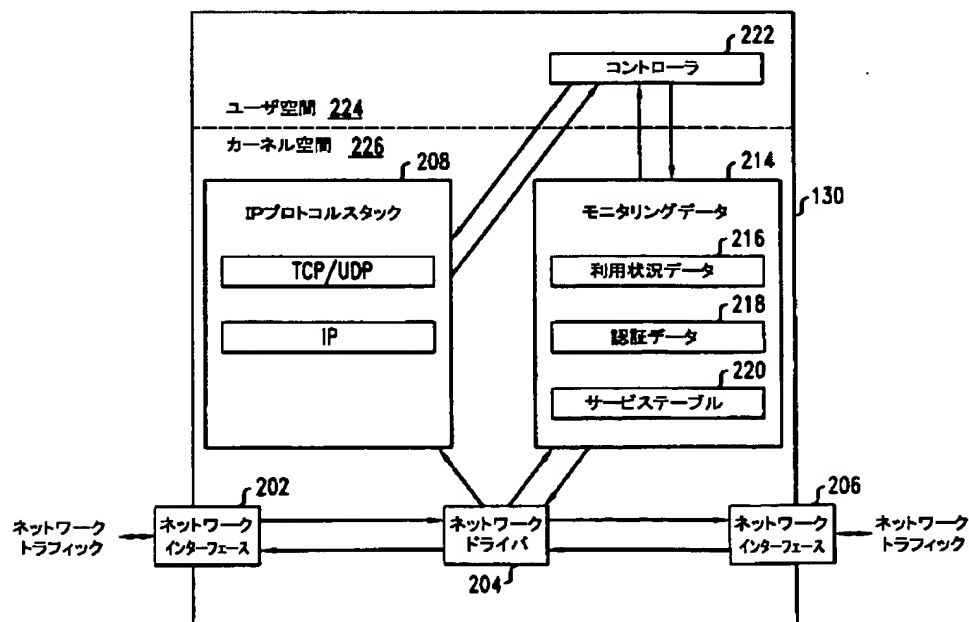
322 タイプフィールド  
 324 ユーザIDフィールド  
 326 サービスタイプフィールド  
 328 IPアドレスフィールド  
 330 サービスフィールド  
 402 IPアドレスフィールド  
 404 マスクフィールド  
 406 プロトコルフィールド  
 408 ポートフィールド  
 410 ユーザフィールド  
 412 ドメインフィールド  
 414 タイプフィールド  
 416 ユーザIDフィールド

502 IPアドレスフィールド  
 504 マスクフィールド  
 506 プロトコルフィールド  
 508 ポート範囲フィールド  
 600 データパケット  
 602 IPヘッダ  
 604 TCPヘッダ  
 606 TCPデータ  
 608 プロトコルフィールド  
 610 ソースIPアドレスフィールド  
 612 デスティネーションIPアドレスフィールド  
 614 ソースポートフィールド  
 616 デスティネーションポートフィールド

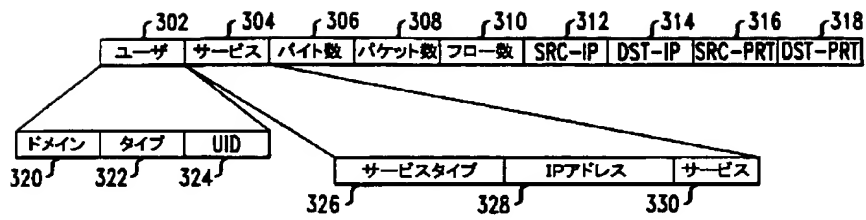
【図1】



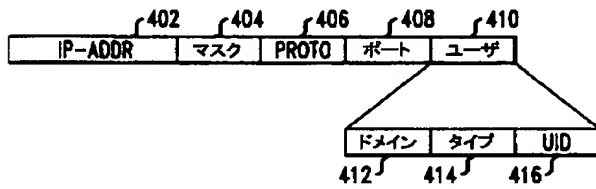
【図2】



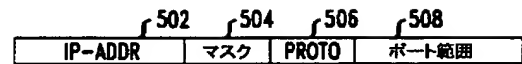
【図 3】



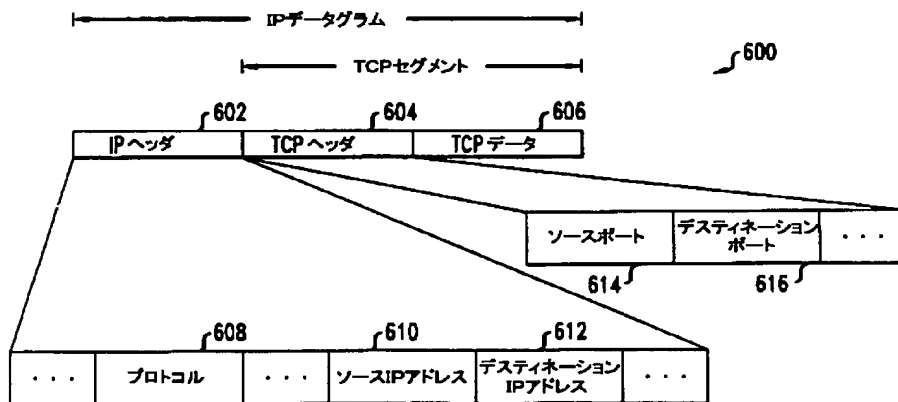
【図 4】



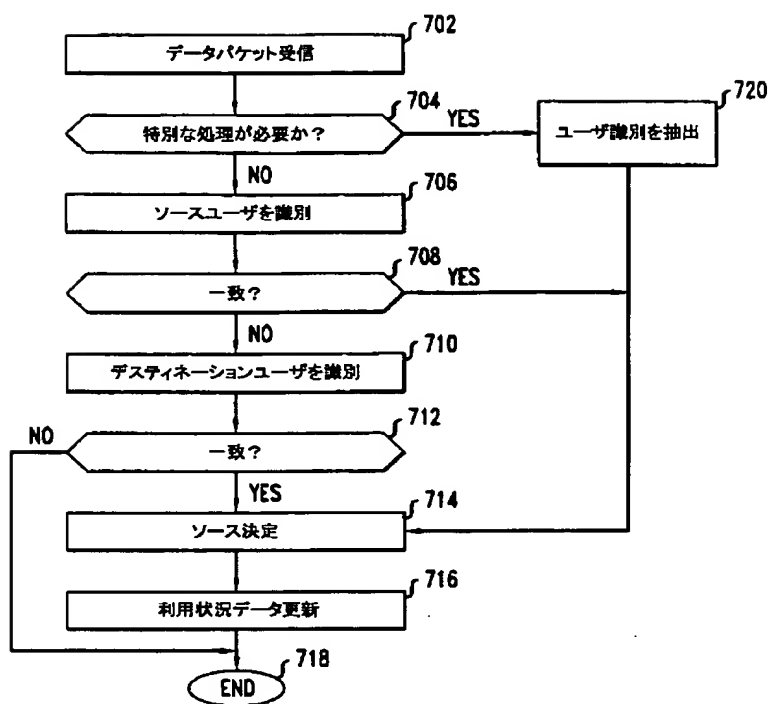
【図 5】



【図 6】

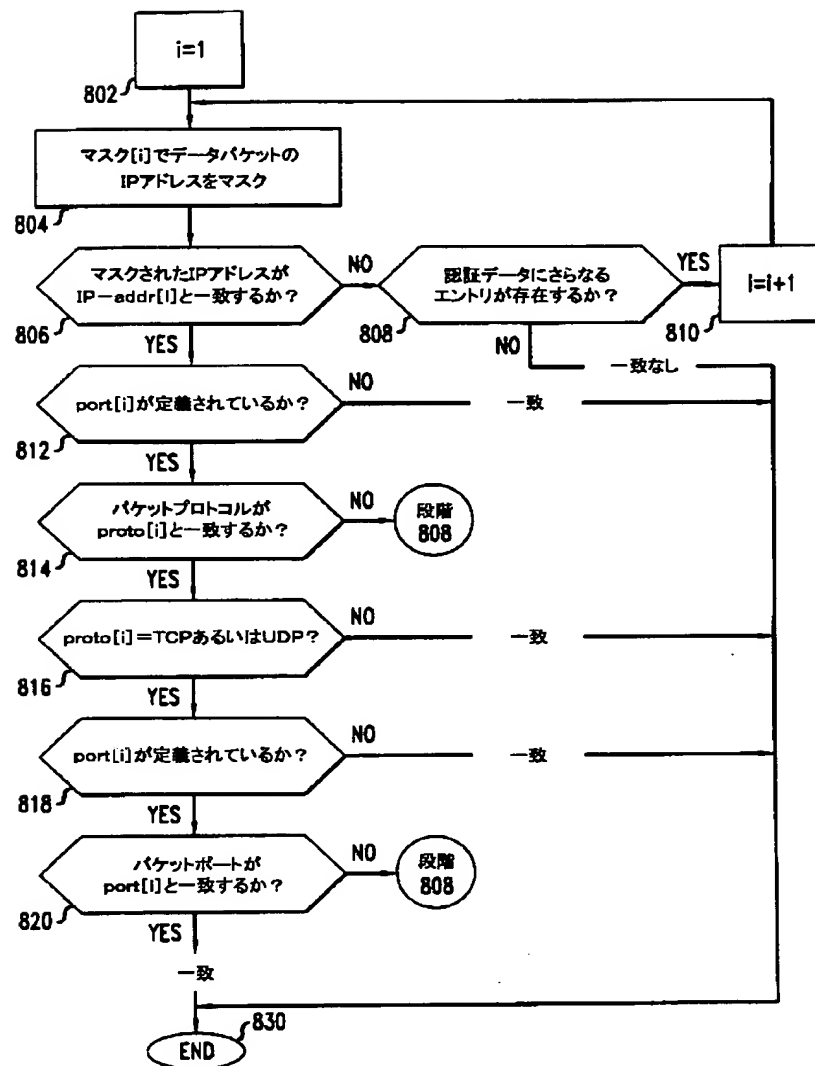


【図 7】

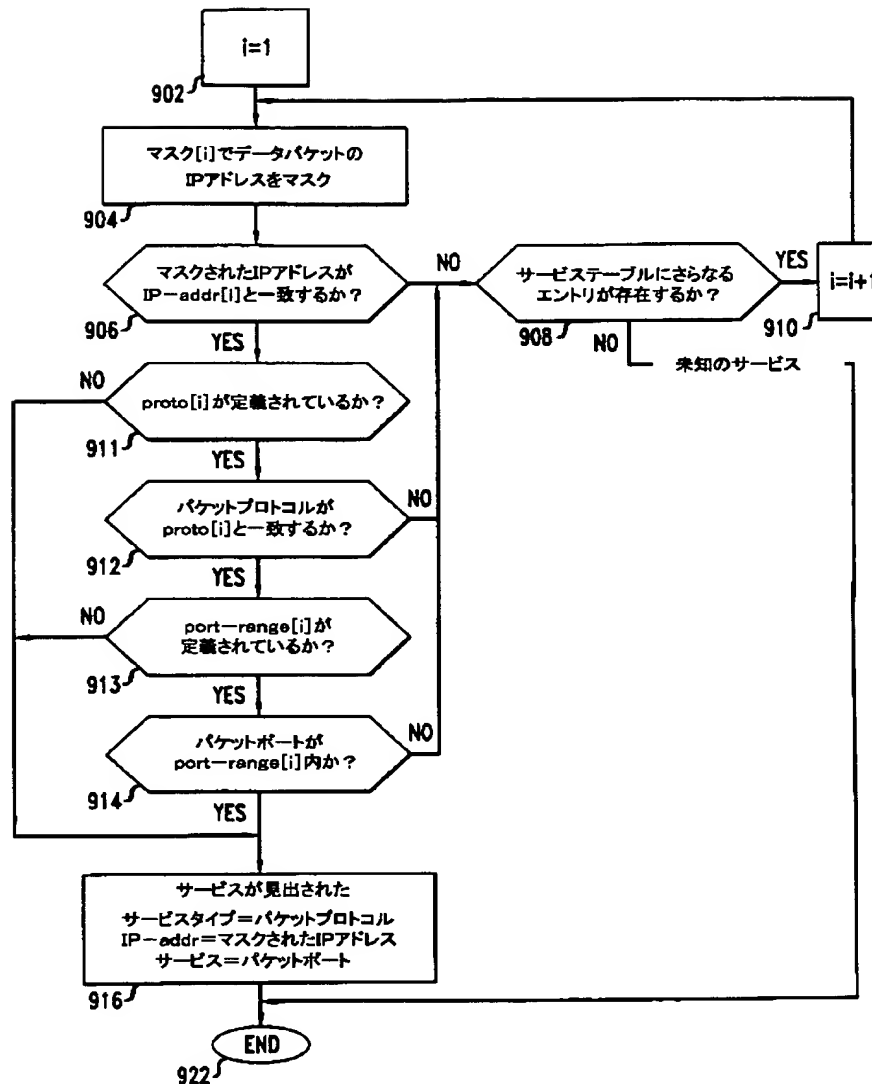




【図8】



【図 9】



フロントページの続き

(51) Int. Cl.<sup>7</sup>

G 0 6 F 15/177

H 0 4 L 12/56

識別記号

6 7 2

F I

G 0 6 F 15/177

H 0 4 L 11/20

テーマコード(参考)

6 7 2 C

1 0 2 A

(71) 出願人 596077259

600 Mountain Avenue,  
Murray Hill, New Je  
rsey 07974-0636 U. S. A.

(72) 発明者 ステファン マイケル プロット  
アメリカ合衆国、07901 ニュージャージ  
ー、ジレット、ロング ヒル ロード

384

(72) 発明者 ユリ ブライトバート

アメリカ合衆国、07940 ニュージャージ  
ー、マディソン、フェアファックス コ  
ート 90

(72) 発明者 クリフォード イー、マーチン  
アメリカ合衆国、08836 ニュージャージ  
ー、マーチンスビル、エヌ、ボッセラー  
アベニュー 802

**拒絶理由通知書**

特許出願の番号	特願2000-050476
起案日	平成15年 8月 7日
特許庁審査官	小林 紀和 4240 5X00
特許出願人代理人	丸山 隆夫 様
適用条文	第29条の2

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から60日以内に意見書を提出して下さい。

**理 由**

この出願の請求項 1-14 に係る発明は、その出願の日前の出願であって、その出願後に公開された下記 1, 2 の出願の願書に最初に添付した明細書又は図面に記載された発明と同一であり、しかも、この出願の発明者がその出願前の出願に係る上記の発明をした者と同一ではなく、またこの出願の時に於いて、その出願人がその出願前の出願に係る上記特許出願の出願人と同一でもないため、特許法第29条の2の規定により特許を受けることができない。

**記**

1. 特願2000-148684号(特開2001-44992号)
  2. 特願平10-232440号(特開2000-069017号)
- (備考)

引例1の段落12, 13、図1を参照。

引例2の請求項1を参照。

**先行技術文献調査結果の記録****・調査した技術分野**

国際特許分類第7版(IPC 7): H04L 12/

Fタームテーマ : 5K030(広域データ交換)

この拒絶理由通知書の内容等に関する問い合わせ先

特許審査第四部 デジタル通信(データネットワーク) 小林紀和

電話 (03) 3581-1101 内線3556